UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,615	07/30/2001	Phillip W. Rogaway	ROG01-0002	3083

22835 7590 04/07/2005

A. RICHARD PARK, REG. NO. 41241
PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95616

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/918,615	ROGAWAY, PHILLIP W	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41,50-52 and 61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41,50-52 and 61* is/are rejected.

7)☒ Claim(s) *40,51* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-41,50-52, and 61 have been considered.

Specification

The disclosure is objected to because of the following informalities: the applicant labels Fig 6 as the IAPM cryptographic scheme and Fig 7 as the IACBC cryptographic scheme of Charanjit Jutla. The applicant has got the schemes reversed. Fig 6 is IACBC and Fig 7 is IAPM. See "Encryption Modes With Almost Free Message Integrity" pages 3 and 5 enclosed with the office action. Appropriate correction is required.

The disclosure is objected to because of the following informalities: "offset M[m + 1]" on line 2 of page 8 should be "offset Z[m +1]". Appropriate correction is required.

Claim Objections

Claims 40 and 51 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 41 and 52 recite the limitation "0^{th} basis offset". There is insufficient antecedent basis for this limitation in the claim. Though claims 40 and 51 discuss the construction for a "0^{th} basis offset", neither claims 41 and 52 nor claims 39 and 50 on which claims 41 and 52 depend discuss a "0^{th} basis offset" or how such an offset is created or implemented in the system. As such the applicant's reference to a "0^{th} basis offset" lacks antecedent basis in the claims. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-6,8-9,13-15,19-24,26-27,31-33, and 37-38 are rejected under 35 U.S.C. 102(e) as being anticipated by Gligor, U.S. Patent No. 2001/0033656.

As per claims 1,19, and 37, the applicant describes an authenticated-encryption method that uses a key, a nonce and an n-bit block cipher to encrypt a message into a ciphertext, comprising the following limitations which are met by Gligor:

a) partitioning the message into a message body comprising a sequence of n-bit message blocks, and a message fragment of at most n bits (21 of Fig 9; [0025]);

b) generating a sequence of offsets from the nonce and the key (91 of Fig 9);

c) computing a ciphertext body using the block cipher, the message body, the key, the nonce, and the sequence of offsets (22 of Fig 9);

d) computing a ciphertext fragment using the block cipher, the message fragment, the key, and an offset (y4 of 22 of Fig 9);

e) computing a tag as a function of the message body, the message fragment, the sequence of offsets, and the key (y5 of 22 of Fig 9);

f) defining the ciphertext to include the ciphertext body, the ciphertext fragment, and the tag (24 of Fig 9);

The applicant's discloses a parallelizable cryptographic method which is unique in that it provides both data confidentiality and authentication of the sender. Furthermore, Gligor discloses an authenticated-encryption method which solves the same problem the applicant attempts to solve of providing data confidentiality and integrity of a message.

Referring to Fig 9, the block cipher is 40, the encryption key is 31, the message body is x1, x2, and x3, the message fragment is x4, the ciphertext body is y1, y2, and y3, the ciphertext fragment is y4, the tag is y5, the nonce is 82, and the sequence of offsets is 91. The applicant should also note that the message fragment x4 can be 1 to n bits. If the message fragment is 1 to n-1 bits, it is padded with zeroes to make a complete block of n bits.

As per claims 2 and 20, the applicant describes the method of claims 1 and 19, which are met by Gligor (see above), with the following limitation which is also met by Gligor:

Wherein generating the sequence of offsets involves:

a) determining a first offset as a function of the nonce and the key ([0140], Fig 9);

b) determining each subsequent offset by combining a previous offset and a basis offset, wherein each basis offset is determined as a function of the key ([0140], Fig 9);

The first offset is r_o x 1. Each subsequent offset is a combination of the previous offset with the basis offset, r_o.

As per claims 3-4,15,21-22, and 33, the applicant describes the method of claims 1,14,19, and 32, which are met by Gligor (see above), with the following limitation which is also met by Gligor:

Wherein generating the sequence of offsets involves determining an offset by combining a base offset and a fixed offset, wherein the base offset is a function to the key and the nonce, and the fixed offset is a function of the key and the position of the offset in a sequence of offsets (Fig 9);

The base offset is r_o x 1. The fixed offset is r_o x (i – 1) where i is the position of the offset in the sequence of offsets. For example, for x3, the offset is r_o x 3. r_o x 3 is a combination of the base offset (r_o x 1) and the fixed offset (r_o x 2).

As per claims 5 and 23, the applicant describes the method of claims 4 and 19, which are met by Gligor (see above), with the following limitation which is also met by Gligor:

Wherein the key determines a sequence of basis offsets and each fixed offset is determined by xoring some combination of basis offsets ([0140]);

Modulo 2 addition is an xoring process.

As per claims 6 and 24, the applicant describes the method of claims 5 and 23, which are met by Gligor (see above), with the following limitation which is also met by Gligor:

Wherein each basis offset except for the first basis offset is determined by a shift and a conditional xor applied to a previous offset ([0140]; Fig 9);

For x3, the fixed offset is r_o x 2 which is determined by xoring the base offset with the base offset.

As per claims 8 and 26, the applicant describes the method of claims 1 and 19, which are met by Gligor (see above), with the following limitation which is also met by Gligor:

a) computing a sequence of basis offsets from the key (Fig 9);

b) computing a base offset from the key and the nonce (Fig 9);

c) computing the first offset in the sequence of offsets as a function of the base offset, the key, and the nonce, and computing each subsequent offset in the sequence of offsets by combining the prior offset with a basis offset (Fig 9).

As per claims 9 and 27, the applicant describes the method of claims 9 and 27, which are met by Gligor (see above), with the following limitation which is also met by Gligor:

a) computing a key-variant by enciphering a constant with the block cipher, wherein the block cipher is keyed by the given key (Fig 9);

b) computing the sequence of offsets as a function of the key variant and the nonce (Fig 9);

The key-variant can be r_o (80 of Fig 9) and the block cipher can be the encryption block (70 of Fig 9). The sequence of offsets is a function of the key variant, r_o, and the nonce ctr since the key variant is a function of the nonce and the sequence of offsets is a function of the key variant.

As per claims 13 and 31, the applicant describes the method of claims 1 and 19, which are met by Gligor (see above), with the following limitation which is also met by Gligor:

a) computing a checksum from at least the message (Fig 9);

b) combining the checksum with an offset to produce a precursor full tag (Fig 9);

c) computing a full tag by applying the block cipher to the precursor full tag (Fig 9);

d) computing a tag as a portion of the full tag (Fig 9);

The checksum is the MDC which is an XOR of the x1, x2, x3, and x4. The checksum is combined with the encrypted first offset to produce a precursor full tag. The precursor full tag is fed into the block cipher to produce a full tag. The full tag is combined with the final offset to produce the tag.

As per claims 14, 32, and 38, the applicant describes an authenticated-encryption method that uses a key, a nonce, and an n-bit block cipher to decrypt a ciphertext into a message or a message-invalid signal comprising the following limitations which are met by Gligor:

a) partitioning the ciphertext into a ciphertext body comprising a sequence of n-bit ciphertext blocks, a ciphertext fragment of at most n bits, and a tag (22 of Fig 10);

b) generating a sequence of offsets from the nonce and the key (91 of Fig 10);

c) computing a message body using the block cipher, the ciphertext body, the key, the nonce, and the sequence of offsets (21 of Fig 10);

d) computing a message fragment using the block cipher, the ciphertext fragment, the key, and the offset (21 of Fig 10);

e) computing a new tag with the tag (64 of Fig 10);

f) comparing the new tag with the tag (64 of Fig 10);

g) if the new tag matches the tag, returning the message, wherein the message includes the message body and the message fragment (64 of Fig 10);

h) if the new tag does not match the tag, returning a message-invalid signal (20 of Fig 10).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gligor in view of Press, (Press, William H. Numerical Recipes in C: The Art of Scientific Computing. 1992. Cambridge University Press).

As per claims 7 and 25, the applicant describes the method of claims 5 and 24, which are met by Gligor (see above), with the following limitation which is met by Press:

Wherein the order that basis offsets are combined into fixed offsets is determined according to a Gray code (Press: pages 894-896).

Gligor describes all the limitations of claims 5 and 24. However, Gligor does not describe the use of Gray code.

Press discloses that Gray code can be used to randomize a sequential arrangement. Furthermore, instead of combining the basis offsets with the fixed offsets in a sequential order such as in Gligor's system, one could combine the basis offsets with the fixed offsets in a random order based on Gray code for further randomization. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Press with those of Gligor and incorporate the use of Gray code because doing so creates more randomization.

Claims 10,12,16,18,28,30,34, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gligor in further view of Jutla (Jutla, Charanjit. Encryption Modes with Almost Free Message Integrity. August 2000).

As per claims 10,16,28, and 34, the applicant describes the method of claims 1,14,19, and 32, which are met by Gligor (see above), with the following limitations which are met by Gligor in view of Jutla:

a) combining each message block in the message body with a corresponding offset to produce a corresponding input block (Jutla: Fig 2, page 5);

b) applying the block cipher to each input block to produce a corresponding output block (Gligor: Fig 9);

c) combining each output block with a corresponding offset to produce a corresponding ciphertext block (Gligor: Fig 9);

d) concatenating the ciphertext blocks to determine the ciphertext body (Gligor: Fig 9);

Gligor describes all the limitations of claims 1,14,19, and 32. Gligor also describes parts b) through d) of the claim above. However, Gligor does not describe that an offset is combined with the message block before the block cipher.

Jutla discloses an authenticated-encryption method similar to that of the applicant's called IAPM (Integrity Aware Parallelizable Mode). Jutla discloses that an offset (S_i in Fig 2) is combined with a message block before the block cipher. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Jutla with those of Gligor and combine an offset with a message block before the block cipher for further encipherment of a message.

As per claims 12,18,30, and 36, the applicant describes the method of claims 1,14,19, and 32, which are met by Gligor (see above), with the following limitations which are met by Gligor in view of Jutla:

a) computing a checksum as a function of the message, the ciphertext fragment, and the sequence of offsets (Gligor: Fig 9; Jutla: Fig 1 of page 3);

b) computing the tag as a function of the checksum, the key, and an offset (Gligor: Fig 9);

Gligor discloses all the limitations of claims 1,14,19, and 32. Gligor also discloses part b above and the computation of a checksum based on the message and a sequence of offsets (see rejection for claim 1). However, Gligor does not that the checksum is computed based on the ciphertext fragment.

Jutla discloses a cryptographic method similar to IAPM (discussed in the rejection for claim 10) called IACBC (Integrity Aware Cipher Block Chaining). In this method, Jutla discloses that the tag (C_m) is computed based on a checksum being fed into a block cipher which incorporates the ciphertext fragment. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Jutla with those of Gligor and incorporate the use of the ciphertext fragment in the generation of the checksum because doing so creates further encipherment.

Claims 11,17,29,35,39,50, and 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gligor in view of Jutla in further view of Menezes, (Menezes, Alfred J. Handbook of Applied Cryptography. 1997. CRC Press. Pages 321-383).

As per claims 11,17,29, and 35, the applicant describes the method of claims 1,14,19, and 32, which are met by Gligor (see above), with the following limitations which are met by Gligor in view of Jutla in further view of of Menezes:

a) computing a precursor pad as a function of an offset and the length of the message (Gligor: Fig 9; Jutla: Fig 2, page 5);

b) computing a pad by applying the block cipher to the precursor pad (Gligor: Fig 9);

c) computing the ciphertext fragment by combining the message fragment and the pad (Menezes: page 340);

Gligor discloses all the limitations of claims 1,14,19, and 32. The applicant should note that the precursor pad is computed as a function of the length of the message because the precursor pad is the

same length as a message block. Gligor, however, does not disclose that the message fragment is combined with the pad to form the ciphertext fragment and that an offset is combined to form a precursor pad before the block encipherment.

Menezes discloses combining the ciphertext fragment with the pad. Menezes discloses a block ciphering method known as Matyas-Meyer-Oseas in which an input message is combined with the result of a block cipher process to form a ciphertext. Combining the ideas of Menezes with those of Gligor would allow x4 to be combined at 92 with z4.

Jutla discloses computing a precursor pad as a function of an offset (see the rejection for claim 10).

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Jutla and Menezes with those of Gligor because doing so allows for further encipherment.

As per claims 39,50, and 61, the applicant describes an authenticated-encryption method that uses an n-bit block cipher, a key, and an n-bit nonce to encrypt a message into a ciphertext comprising the following limitations which are met by Gligor in view of Jutla in further view of Menezes:

a) partitioning the message into me message blocks and one final fragment, each message block having n bits and the final fragment having between 0 and n bits (Gligor: Fig 9);

b) using the block cipher, the key, and the nonce to generate a sequence of m offsets, each offset having n bits (Gligor: Fig 9);

c) using the block cipher, the key, the nonce, and the length of the message to generate an n-bit final offset (Gligor: Fig 9);

d) for each i between l and m, xoring the ith message block with the ith offset to determine an ith input block (Jutla: Fig 2 of page 5);

e) for each number i between l and m, applying the block cipher, keyed by the key, to the ith input block, to determine an ith output block (Jutla: Fig 2 of page 5);

f) for each number I between I and m, xoring the ith output block with the ith offset to determine an ith ciphertext block (Jutla: Fig 2 of page 5);

g) concatenating the m ciphertext blocks to determine a ciphertext body (Gligor: Fig 9);

h) computing an encoded length by encoding the length of the final fragment as an n-bit string (Jutla: [0025]);

i) xoring the encoded length with the final offset to determine a precursor pad (Gligor: Fig 9; Jutla: Fig 2 of page 5);

j) computing a pad by applying the block cipher, keyed by the key, to the precursor pad (Gligor: Fig 9);

k) xoring the final fragment with a portion of the pad to determine a ciphertext fragment having the same length as the final fragment (Menezes: page 340);

l) computing a padded ciphertext fragment by appending to the ciphertext fragment a sufficient number of zero bits so that the padded ciphertext fragment has n bits (Gligor: [0025]);

m) computing a checksum by xoring together the m message blocks, the pad, and the padded ciphertext fragment (Gligor: Fig 9);

n) computing a precursor full tag by xoring together the checksum and the mth offset (Gligor: Fig 9);

o) determining a full tag by applying the block cipher, keyed by the key, to the precursor full tag (Gligor: Fig 9);

p) computing a tag as a portion of the full tag (Gligor: Fig 9);

q) defining the ciphertext to be the ciphertext body, the ciphertext fragment, and the tag (Gligor: Fig 9);

All the limitations have been discussed throughout the rejection for claims 1-38 and will not be repeated.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

***